REMARKS

Upon entry of this Amendment, claims 36-70 remain pending and under current examination. The claim amendments will be discussed below with respect to the individual rejections. In the Office Action, the Examiner took the following actions:

(a) rejected claims 37, 39, 44, 46, 47, 49, 54, 56, 61, 63, 64, and 66 under 35 U.S.C. § 112, second paragraph, as being indefinite;

(b) rejected claims 53-70 under 35 U.S.C. § 101 as being directed to non-statutory subject matter;

(c) rejected claims 36-39, 50, 51, 53-56, 67, 68, and 70 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0046275 ("Crosbie"); and

(d) rejected claims 40-49, 52, 57-66, and 69 under 35 U.S.C. § 103(a) as being unpatentable over Crosbie in view of U.S. Patent No. 7,181,768 ("Ghosh").

Applicants respectfully traverse these rejections for the following reasons.

Rejection under 35 U.S.C. § 112, Second Paragraph:

The Office Action rejected claims 37, 39, 44, 46, 47, 49, 54, 56, 61, 63, 64, and 66 as allegedly being indefinite, and particularly, for allegedly lacking antecedent basis. *See* Office Action, pp. 2-3. In response to this rejection, and without conceding to the Office Action's assertions, Applicants have amended these claims to ensure conformance with 35 U.S.C. § 112, second paragraph. Applicants therefore respectfully request withdrawal of this rejection.

Rejection of Claims 53-70 under 35 U.S.C. § 101:

The Office Action alleged that claims 53-70 "comprise recitations directed towards software per se." Office Action, p. 4. Applicants respectfully disagree, and point out that the Office Action misinterpreted the claimed invention. For example, independent claim 53 recites "[a]n apparatus for monitoring operation of a processing system," which is clearly not just "software." This is also clearly explained in the specification at, for example, pp. 8-11, which discusses that the apparatus has "model" and "real system" components. Applicants' claimed "apparatus" is clearly statutory under 35 U.S.C. § 101. Therefore, independent claim 53 should be allowable. Claims 54-69 should also be allowable, at least by virtue of their dependence from base claim 53. Thus, Applicants respectfully request withdrawal of the 35 U.S.C. § 101 rejection of claims 53-69.

Regarding claim 70, and without conceding to the Office Action's assertions regarding allegedly non-statutory subject matter, Applicants have amended the claim to recite a computer readable medium encoded with a computer program product. This amendment overcomes the 35 U.S.C. § 101 rejection, and Applicants accordingly respectfully request its withdrawal.

Rejection of Claims 36-39, 50, 51, 53-56, 67, 68, and 70 under 35 U.S.C. § 102(b):

Applicants request reconsideration and withdrawal of the rejection of claims 36-39, 50, 51, 53-56, 67, 68, and 70 under 35 U.S.C. § 102(b) as being anticipated by Crosbie.

In order to establish anticipation under 35 U.S.C. § 102 , the Examiner must show that each and every element as set forth in the claim is found, either expressly or inherently described, in Crosbie. *See* M.P.E.P. § 2131. Crosbie, however, does not disclose each and every element of Applicants' claims. Specifically, Crosbie does not disclose or suggest at least Applicants' claimed "the step of monitoring, for at least two processes in said plurality, a set of system

primitives that allocate or release said system resources," as recited in independent claim 36 (emphases added, independent claim 53 containing similar recitations).

In contrast, Crosbie discloses a host-based intrusion detection system (IDS) to be run regularly (for example, on a weekly basis) on one or more host systems. *See* Crosbie, par. [0114]. Further, Crosbie's IDS monitors two kinds of log files, namely, kernel audit log files and system log files, to provide intrusion detection. *See* Crosbie, pars. [0115-0117]. However, Crosbie's IDS does not monitor "processes" "running" on a process system, as recited in claims 36 and 53. Rather, Crosbie's IDS operates based on, for example, a weekly schedule and utilizes stored data in log files. *See* Crosbie, pars. [0114-0117].

Moreover, Crosbie's IDS does not require a specific type of system calls to perform intrusion detection. For example, Crosbie discloses that "[t]he kernel audit logs generally include all the information about every system call executed on the host." Crosbie, par. [0116] (emphases added). In contrast, Applicants' claims 36 and 53 recite "a set of system primitives that allocate or release said system resources" (emphasis added), which does not include all the information about every system call.

Since Crosbie does not disclose each and every element of independent claim 36, Crosbie does not anticipate Applicants' independent claim 36 under 35 U.S.C. § 102(b). Therefore, independent claim 36 should be allowable over Crosbie. Independent claim 53, while of different scope, contains similar recitations as independent claim 36, and should also be allowable for the same reasons as independent claim 36. In addition, dependent claims 37-39, 50, 51, 54-56, 67, 68, and 70 should be allowable at least by virtue of their respective dependence from independent claim 36 or 53. Accordingly, Applicants respectfully request withdrawal of the 35 U.S.C. § 102(b) rejection.

Rejection of Claims 40-49, 52, 57-66, and 69 under 35 U.S.C. § 103(a):

Applicants request reconsideration and withdrawn of the rejection of claims 40-49, 52, 57-66, and 69 under 35 U.S.C. § 103(a) as being unpatentable over Crosbie in view of Ghosh. No *prima facie* case of obviousness has been established with respect to these claims for at least the reason that Crosbie and Ghosh, taken alone or in combination, do not teach or suggest each and every claim element. The burden thus remains with the Examiner.

As explained above, Applicants have established that Crosbie does not disclose or suggest at least Applicants' claimed "the step of monitoring, for at least two processes in said plurality, a set of system primitives that allocate or release said system resources," as recited in independent claim 36 (emphases added, independent claim 53 containing similar recitations). Ghosh does not cure the deficiencies of Crosbie. For example, Ghosh discloses an IDS "for detecting application-based attacks." Ghosh, Abstract. Ghosh further discloses that during data collection and pre-processing phase, application data are collected from audit logs. *See* Ghosh, col. 6, ll. 20-25. More specifically, "the logs comprise a sequential listing of system instructions passed from the application to the operating system." Ghosh, col. 6, ll. 27-29 (emphasis added). That is, in the pre-processing phase, the data are (1) collected from log files; and (2) only application-to-system instructions. Although in the monitoring phase, Ghosh's IDS captures and analyzes audit data in real-time, the audit data are still from log files. *See* Ghosh, col. 10, ll. 56-62. The only difference is "[they are] processed as [they are] produced, or as soon thereafter as possible." *Id.* This is clearly different from Applicants' claimed "step of monitoring, for at least two processes in said plurality, a set of system primitives that allocate or release said system resources," as recited in independent claim 36 (emphases added, independent claim 53 containing similar recitations).

Therefore, Crosbie and Ghosh, taken either alone or in combination, fail to teach or suggest every claim element of independent claim 36. Thus, the burden has not been shifted and no *prima facie* case of obviousness has been established with respect to independent claim 36. Independent claim 36 should therefore be allowable over Crosbie and Ghosh. Independent claim 53, while different in scope, contains similar recitations as independent claim 36, and should also be allowable for the same reason as independent claim 36. Therefore, dependent claims 40-49, 52, 57-66, and 69 should be allowable at least by virtue of their respective dependence from independent claim 36 or 53. Accordingly, Applicants respectfully request withdrawal of the 35 U.S.C. § 103(a) rejection.

Conclusion:

Applicants request reconsideration of the application and withdrawal of the rejection. Pending claims 36-70 are in condition for allowance, and Applicants request a favorable action.

The Office Action contains a number of statements reflecting characterizations of the related claims. Regardless of whether any such statements are identified herein, Applicants decline to automatically subscribe to any such statements or characterizations in the Office Action.

If there are any remaining issues or misunderstandings, Applicants request the Examiner telephone the undersigned representative to discuss them.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: April 7, 2009

By: _____

David M. Longo
Reg. No. 53,235

/direct telephone: (571) 203-2763/